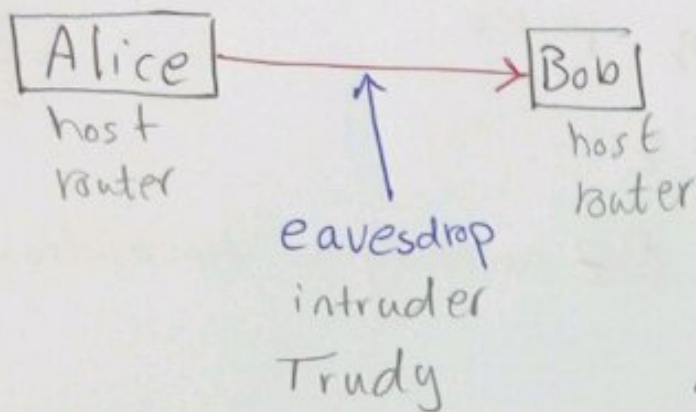


22/3/2017

الأربعاء

داريم

محاضرة [3]



لدي security ؟

① إمكانية sniffing على مكان
confidentiality و privacy

② إمكانية قطع الاتصال وإعتقال ال sender ،
منهم نفسه ال source ؟

* عناصر أمان كدوم ال confidentiality و privacy و integrity
* ضمان الشخص ببياناته قبل ال Authentication

* المعايير :

- هل التامية يؤدي الغرض ؟
- الوقت التي ينفذه التامية ؟

هناك نظامين : Symmetric

↓
فكاح سري
مستعمل بين
الطرفين

Asymmetric

يكون كل شخص له فكاك يفك
عبارة عن Private و public key

- ال Brute force يحاول جدا لللايين
السنين

- سريع في الباب وبسيط
- ينفع للبيانات الكثير

Chapter 8: Network Security

* slide 8.4 , 8.5

* slide 8.7

* Breaking Encryption Scheme 8.10

* RSA algorithm

$$p, q = n$$

choose p, q prime

$$(p-1)(q-1) = z$$

generate z

$$e \cdot d \bmod z = 1$$

choose e & d according to the relation

$$m^e \bmod n = c \quad \text{encrypt}$$

$$c^d = m^{ed} \bmod n \Rightarrow m \quad \text{decrypt}$$

Why does RSA work? 8.25

* Authentication 8.31

* Digital Signatures 8.44